

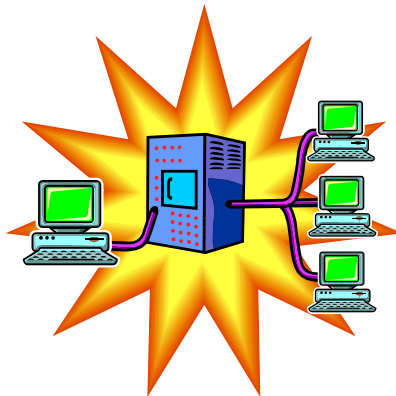


DoD PKI

Server Certificate

Enabling For

Microsoft Internet Information Server 5.0
Step 2: Obtaining/Installing PKI Server Certificate



DoD PKI

Server Certificate

Enabling For

Microsoft Internet Information Server 5.0

Step 2: Obtaining/Installing PKI Server Certificate

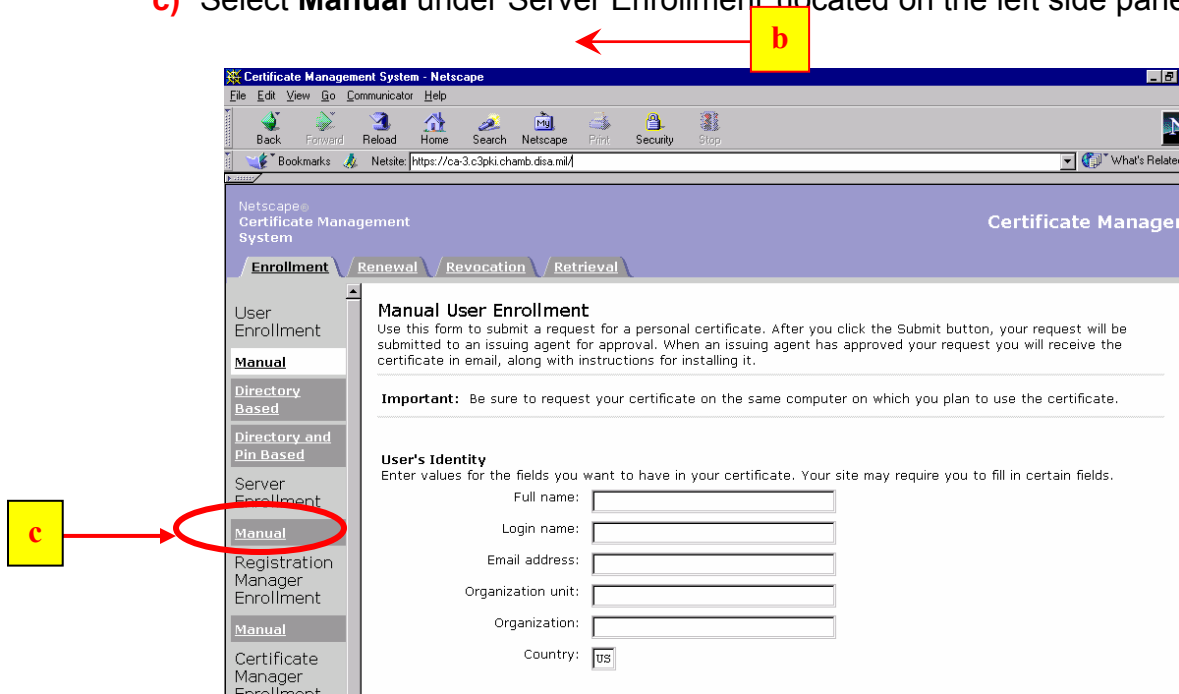
This Document is a follow up to “Server Certificate Enabling for Microsoft Internet Information Server 5.0 Step 1: Generating a Key Pair and Requesting a Certificate.” It details how to obtain and install a PKI server certificate as well as how to make the web server secure (https).

Obtaining/Installing a PKI Server Certificate

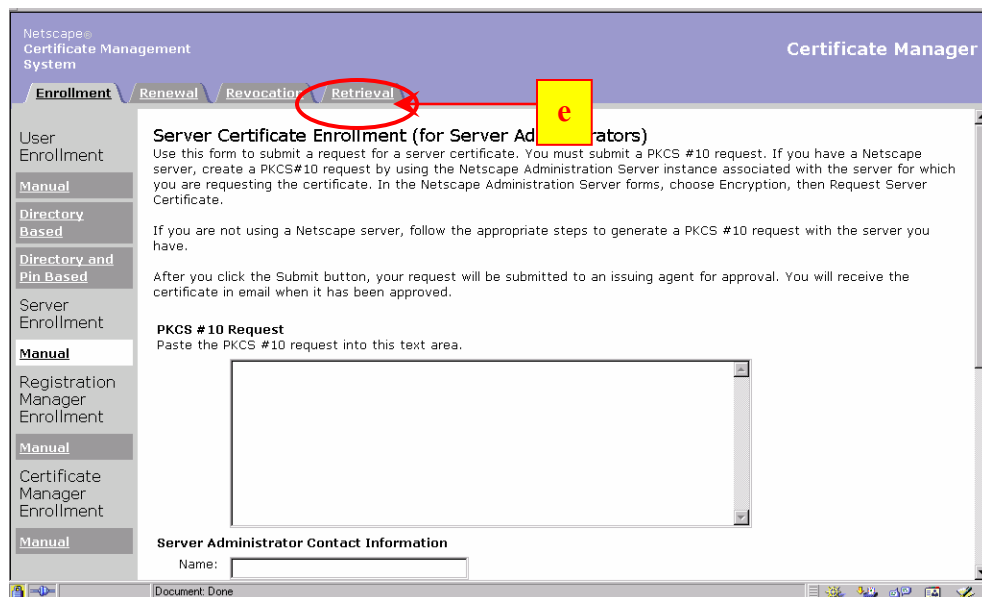
- | | |
|--|---------|
| 1. Obtaining and Installing Certificate/Trusted Chains | Page 3 |
| 2. Installing PKI Certificate/Setting up SSL | Page 8 |
| 3. Installing the Root Certificate Authority | Page 13 |

1. Obtaining/Installing the Certificate.

- a) Open a web browser window this can either be Internet Explorer or Netscape.
- b) Go to site <https://ca-3.c3pki.chamb.disa.mil> and the following page will appear.
- c) Select **Manual** under Server Enrollment (located on the left side pane).



- d) **Server Certificate Enrollment** page will appear.
- e) Click on **Retrieval**.



- f) List Certificates page will appear
- g) Enter the CSN from the email you received into both boxes.
- h) Check the box "Do not show certificates that have been revoked".
- i) Click **Find**

Netscape® Certificate Management System

Certificate Manager

Enrollment Renewal Revocation **Retrieval**

List Certificates

Use this form to list certificates whose serial numbers fall within a specified range.

Enter a range of serial numbers in hexadecimal form (starting with 0x, as in the certificate list) or in decimal form.

Lowest serial number (leave blank for no lower limit)

Highest serial number (leave blank for no upper limit)

☒ Do not show certificates that have been revoked

☒ Do not show certificates that have expired or are not yet valid

First records

- j) Search Results page will appear
- k) Click **Details**.

Netscape® Certificate Management System

Certificate Manager

Enrollment Renewal Revocation **Retrieval**

List Certificates

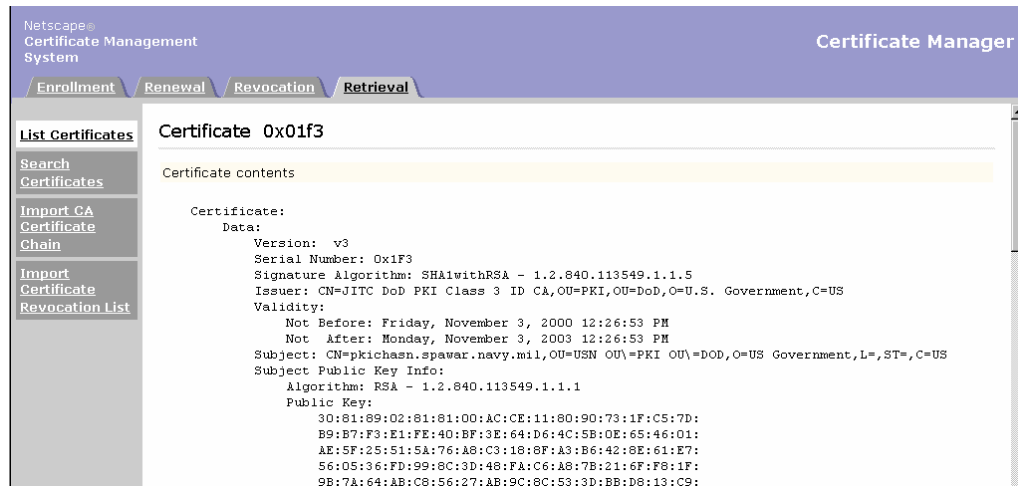
Search Results

Issuer: CN=JITC DoD PKI Class 3 ID CA,OU=PKI,OU=DoD,O=U.S. Government,C=US

Total number of records found: 1

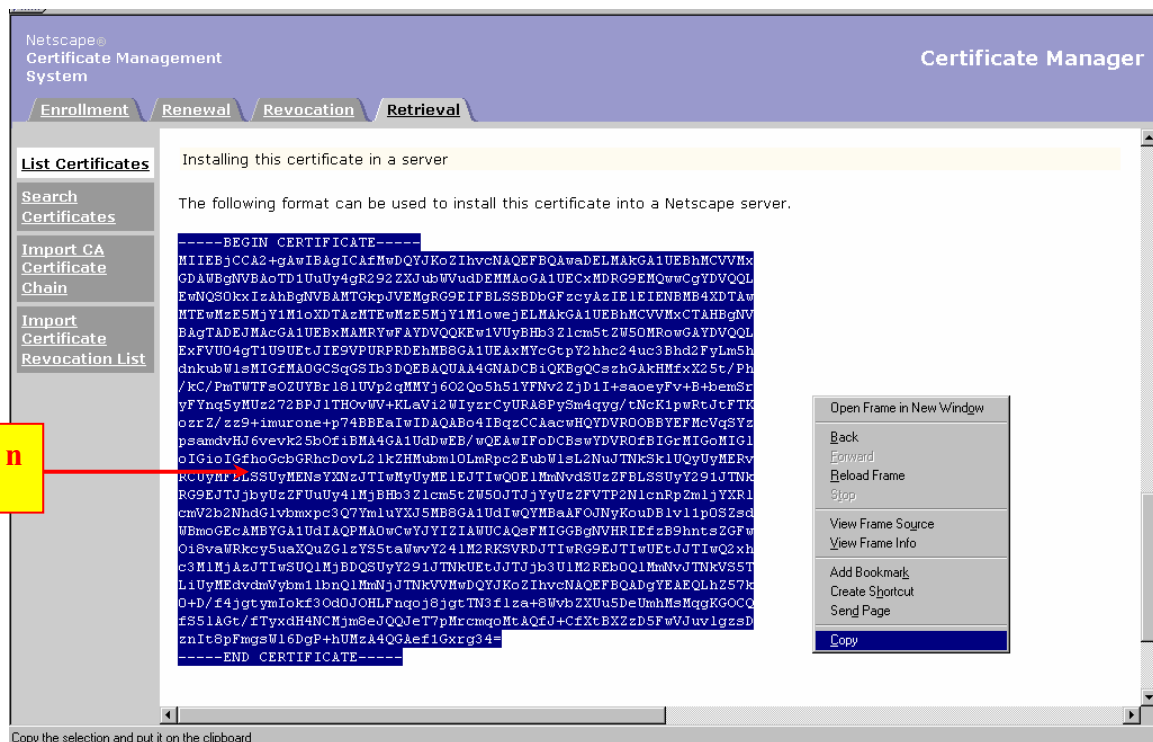
Serial number	Subject name
0x000001f3	CN=pkichasn.spawar.navy.mil, OU=USN OU\=PKI OU\=DOD, O=US Government, L=, ST=, C=US
Version	Subject public key algorithm
3	PKCS #1 RSA with 1024-bit key
Not valid before	Not valid after
11/3/2000	11/3/2003
Issued on	Issued by
11/3/2000	RA.Jensen.Anthony.D.9201000010

I) A Certificate Contents Page will appear.

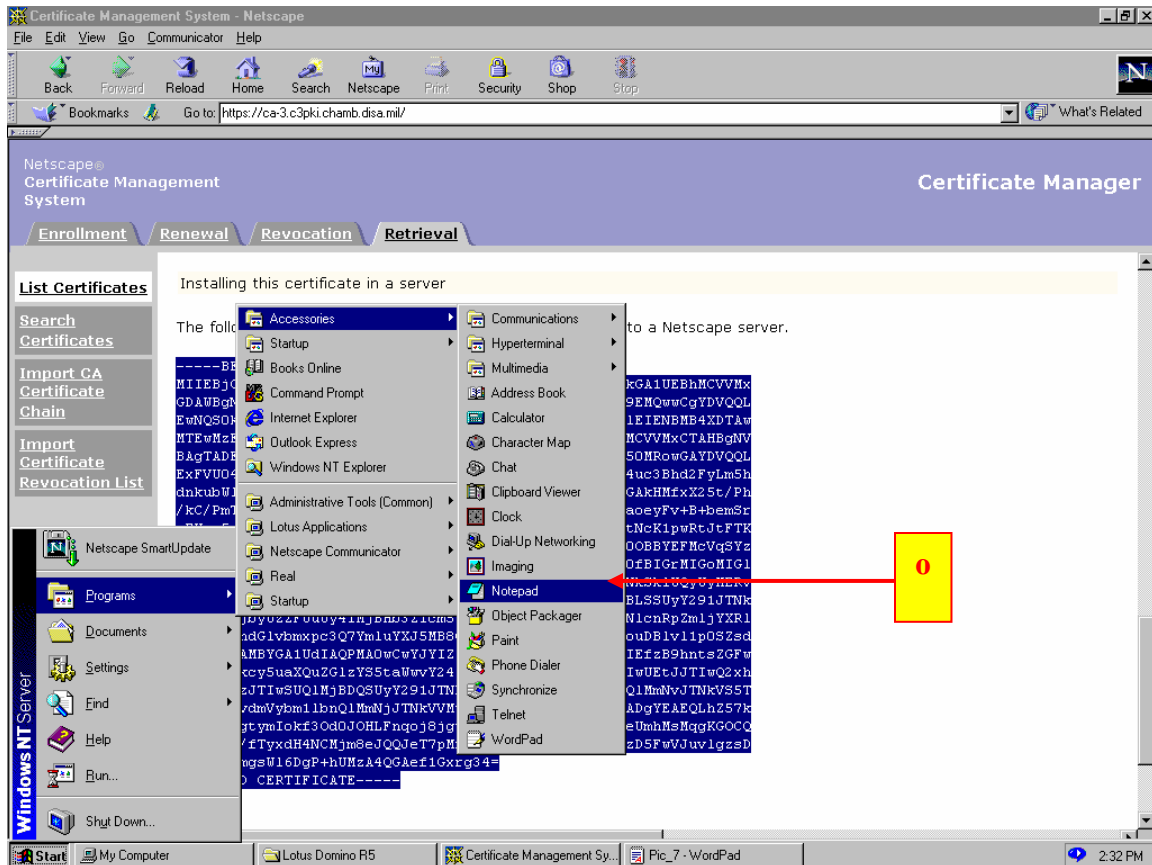


m) Scroll down until “Installing this certificate in a server”.

n) Highlight and copy the Base-64 encoding starting with and including -----**Begin Certificate**----- and ending with the -----**End Certificate**-----.



o) Open Notepad.

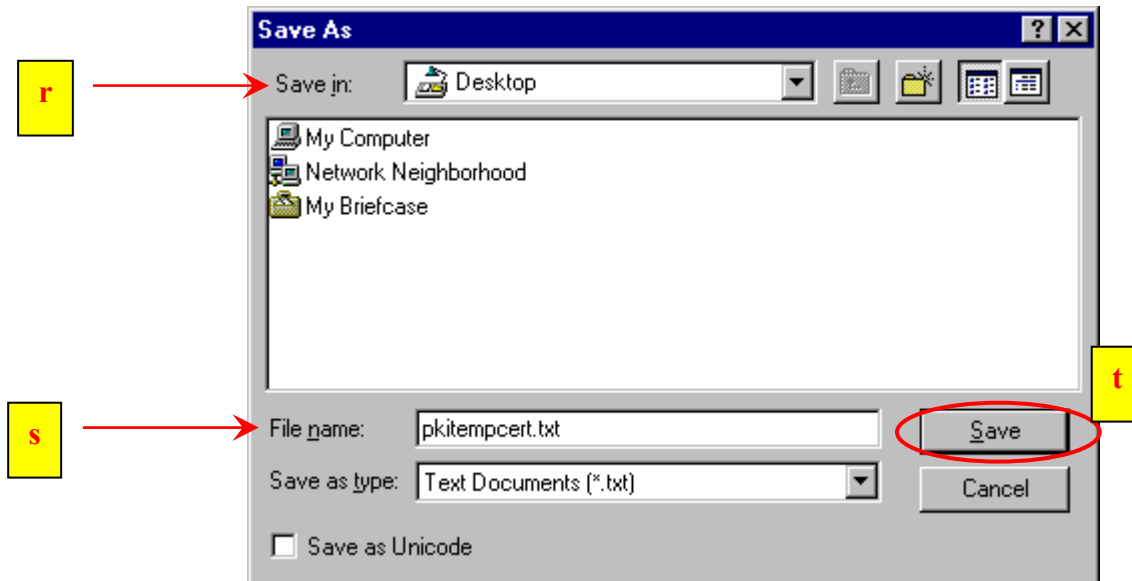


p) sdsdsd

q) Paste the text copied from above to the notepad window. Click **File|Save As**.



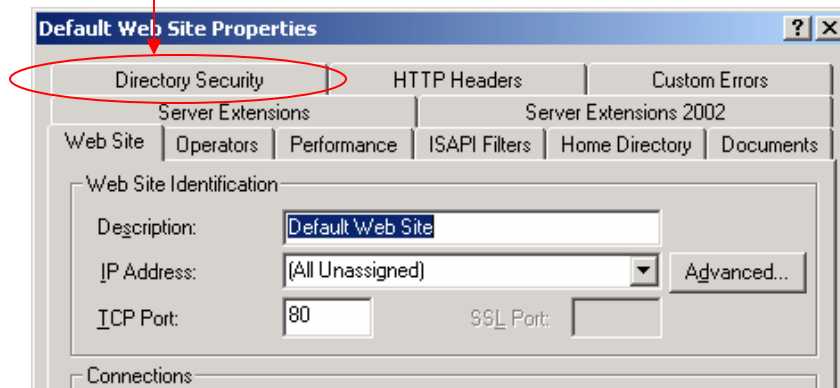
- r) Select **Desktop** in the “Save in:” drop down box.
- s) For filename, use the name **SERVCERT.txt**. (pkitempcert.txt was only an example)
- t) Click **Save**.



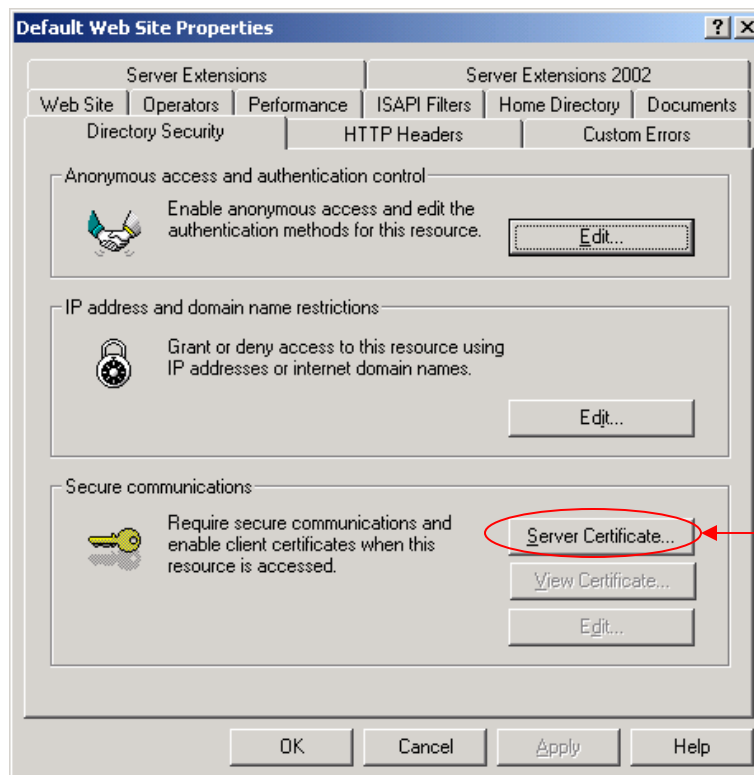
Installing the DoD PKI Certificate in ISS 5.0

You will need to start the **Internet Services Manager**. Click the **Start** button, point at **Programs**, and then point at **Administrative Tools**. From the menu, click **Internet Services Manager**. The **web site Properties** page will display.

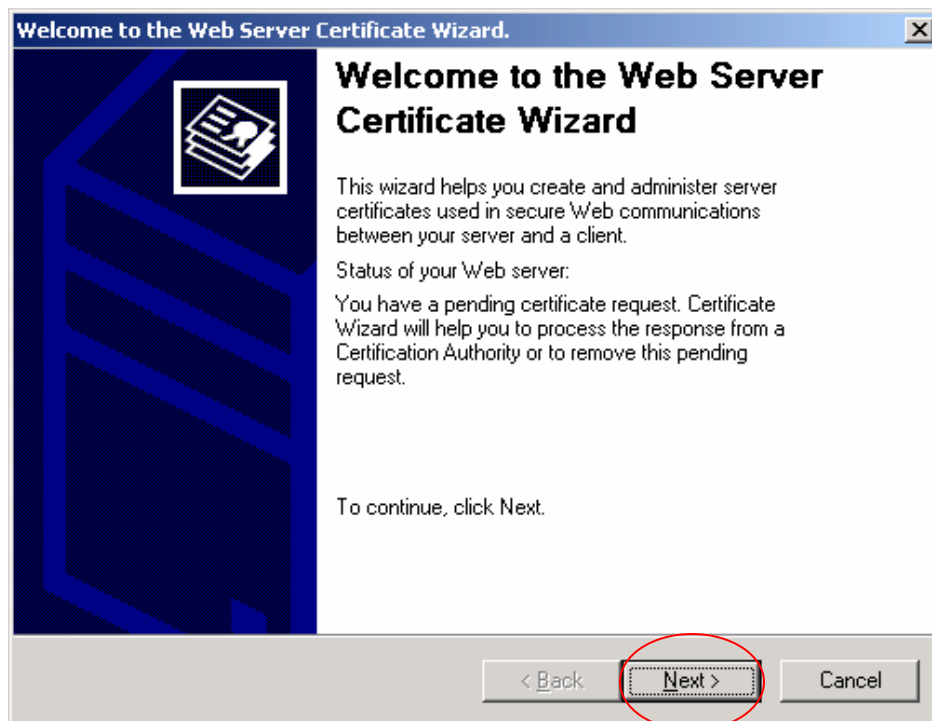
1. Click on **Directory Security** tab.



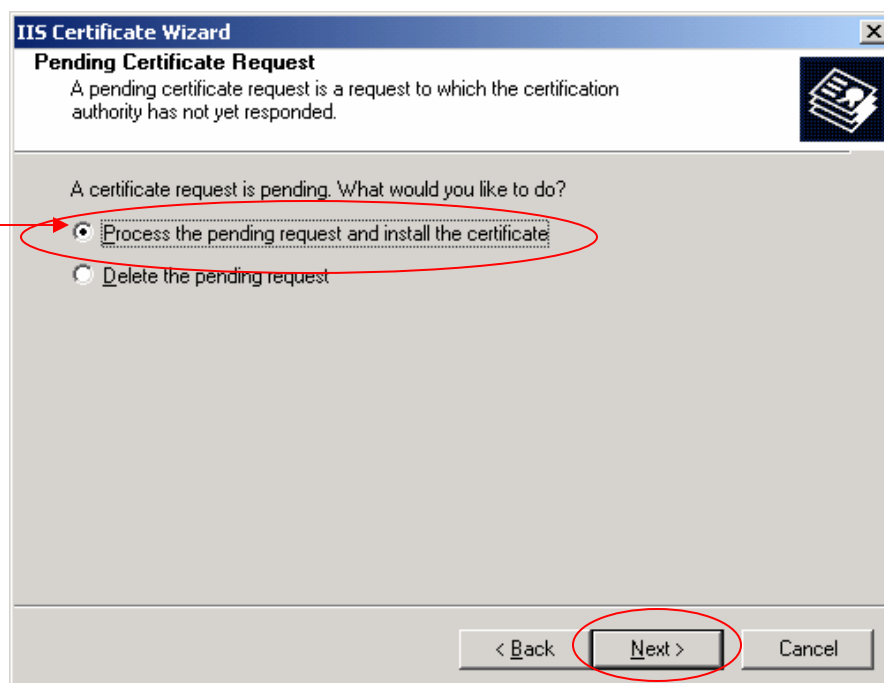
2. Click on **Server Certificate**.



3. The **Welcome to the Web Server Certificate Wizard** page will display. Click on **Next**.

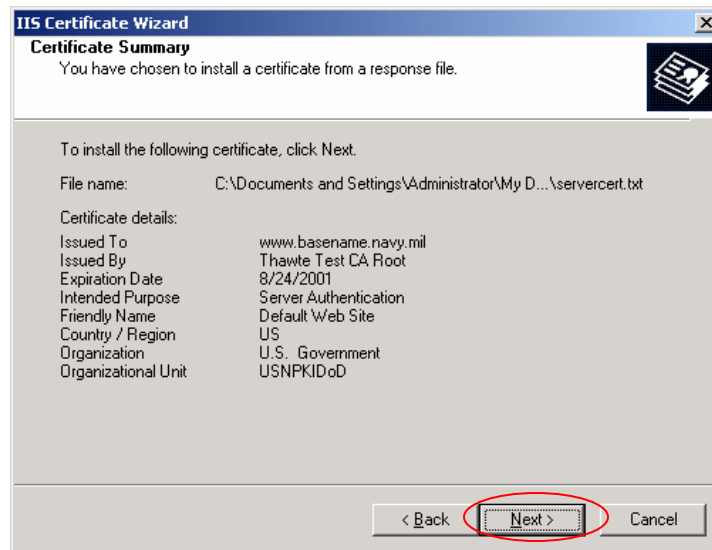


4. Click **Process the pending request and install the certificate**. Click on **Next**.

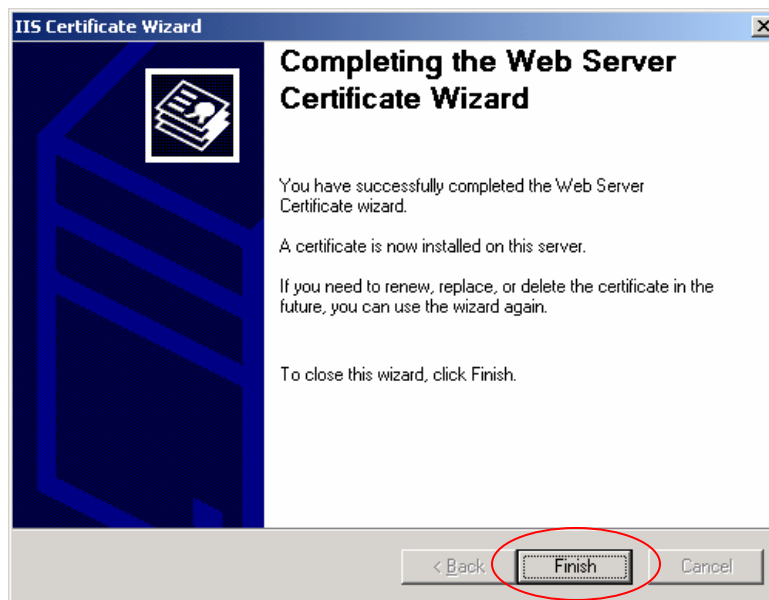


5. Enter the file name and path of the certificate you saved in the previous section. Or, you may click **Browse** to find the certificate. Click **Next** to display the **Certificate Summary** screen.

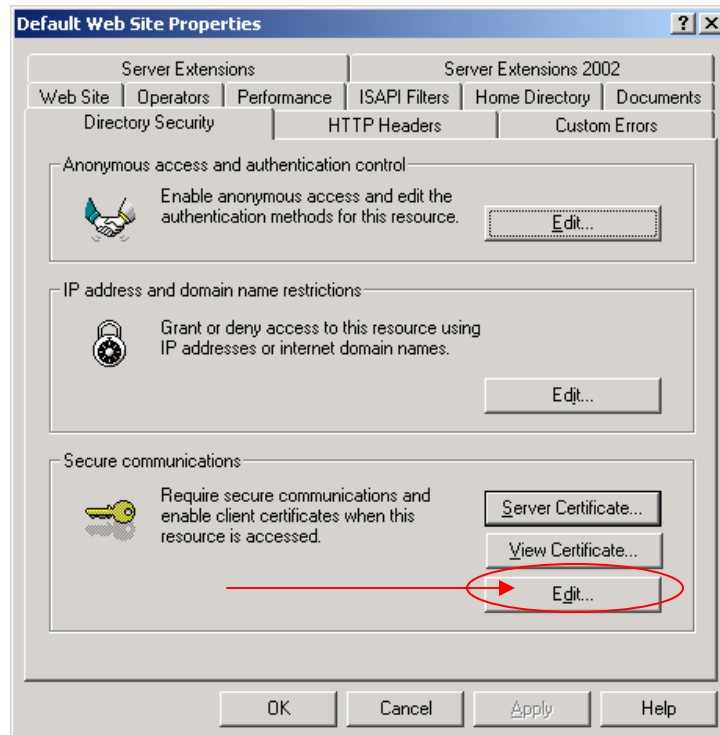
******NOTE:** *If changes need to be made, click **Back** as many screens as needed and make the necessary changes. Click **Next** as many times as needed to return to this screen.*



6. The **Completing the Web Server Certificate Wizard** screen will display. Click on **Finish**.

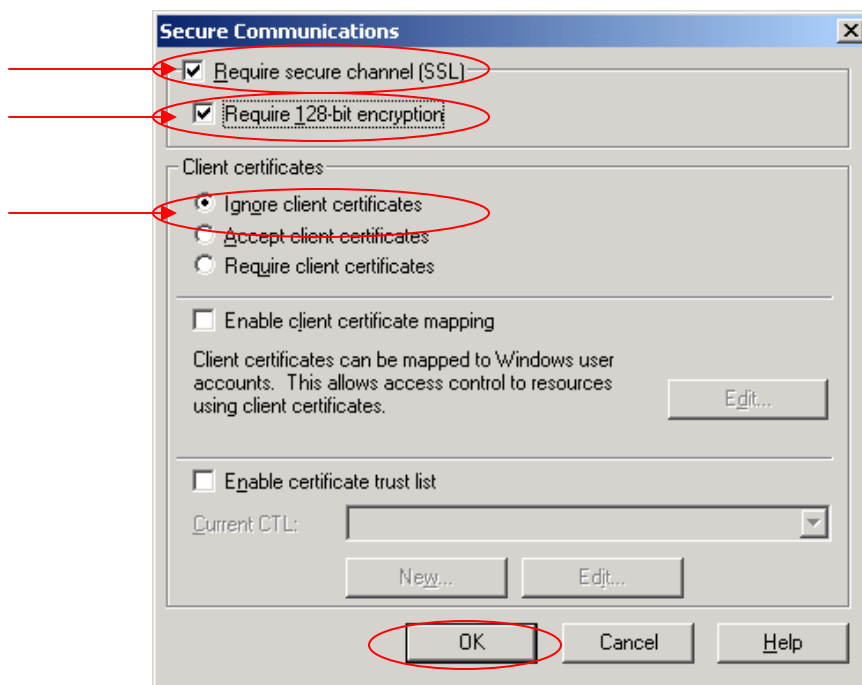


7. You will be returned to the **Edit Secure Communications** screen. Click the **Edit** button.

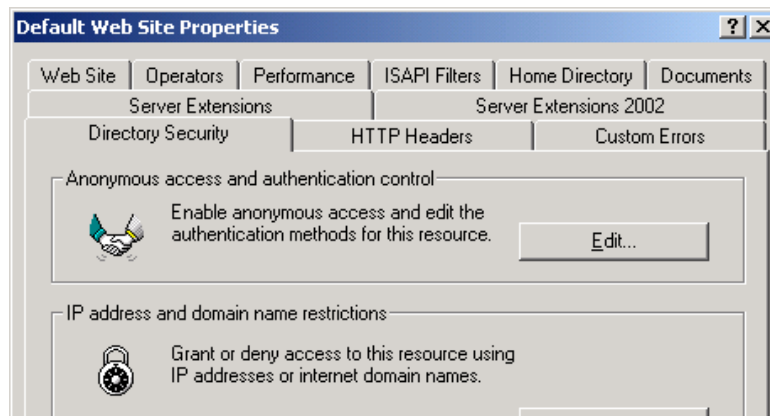


8. Click the **Require Secure Channel (SSL)** box. Also, click **Require 128-bit encryption**. Verify that the **Ignore Client Certificates** button is selected and then click **OK**.

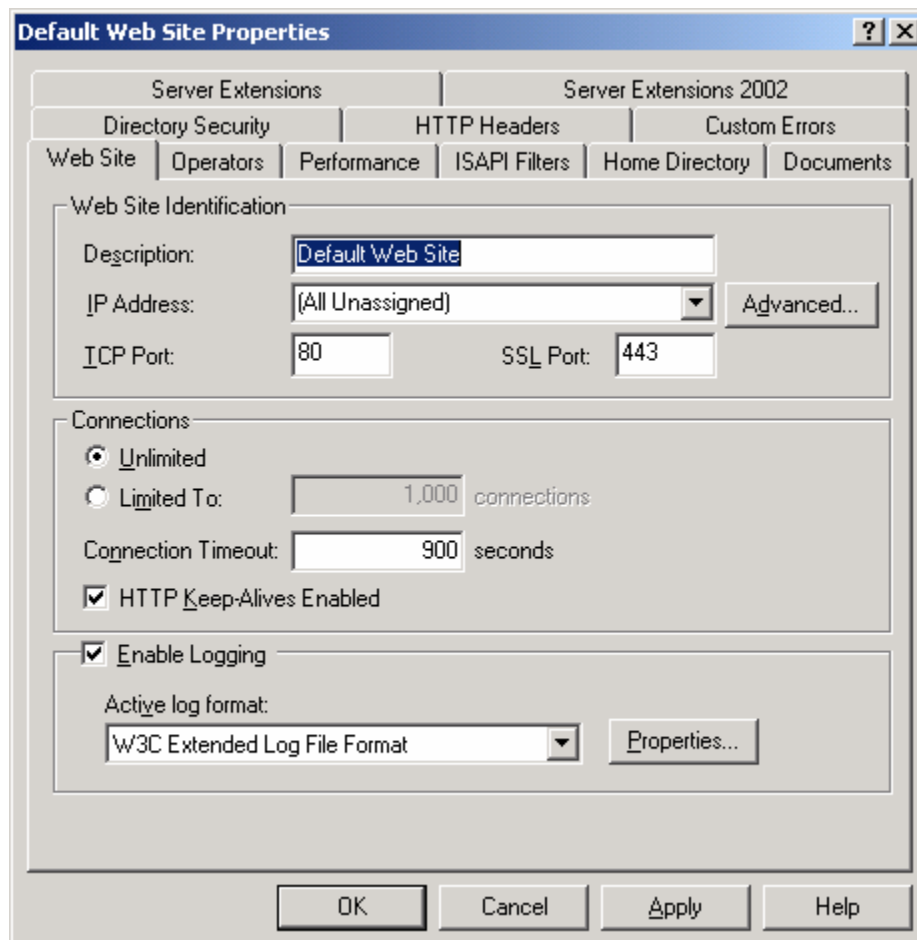
****NOTE: In the DoD implementation, 128-bit encryption algorithms are required.



9. The **Administration Web Site Properties** dialog box appears. Click the **Web Site** tab.



10. In the **SSL Port** field, make sure the number 443 is displayed. You may assign any port number, but port **443** is the default port number for SSL communications. Click **OK**. Close the *Internet Information Manager*. At this point, the web server is SSL-enabled. You may test whether SSL has been activated.



Installing Root Certificate

The final step of the process is to install the Root Authority Certificate onto the Microsoft Certificate Store on the server the web server presides.

Go to https://infosec.navy.mil/NEWPKI/pki_tip.html and follow the instructions for installing all DoD Root Authorities, this is done by use of the Install Root Application.

